

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
7 October 2004 (07.10.2004)

PCT

(10) International Publication Number
WO 2004/086664 A3

(51) International Patent Classification⁷: **H04L 1/00**,
9/00, G06F 11/30

(21) International Application Number:
PCT/IL2004/000144

(22) International Filing Date: 16 February 2004 (16.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
155121 27 March 2003 (27.03.2003) IL
156950 15 July 2003 (15.07.2003) IL

(71) Applicant (for all designated States except US): NDS
LIMITED [GB/GB]; One London Road, Staines, Middle-
sex TW18 4EX (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): BELENKY, Yaacov
[IL/IL]; 27/2 Hakinor Street, Maaleh Adumim 98371 (IL).
SHEN-ORR, Chaim, D. [IL/IL]; 16 Kiryat Sefer Street,
Haifa 34676 (IL).

(74) Agents: SANFORD T. COLB & CO. et al.; P.O. Box
2273, Rehovot 76122 (IL).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,

AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), Euro-
pean (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,
GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments

(88) Date of publication of the international search report:
23 December 2004

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: IMPROVED CFM MODE SYSTEM

(57) Abstract: A method for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K , the method including receiving n plaintext blocks, wherein n is an integer greater than 0, setting Q_0 equal to an initial value, and for each plaintext block of the n plaintext blocks: computing $Q_i = E_K(Q_{i-1}) \text{ XOR } P_i$; and computing $C_i = M(P_i, Q_i)$, thereby producing n ciphertext blocks, wherein $0 < i \leq n$, and P_i denotes an i -th plaintext block of the n plaintext blocks, and C_i denotes an i -th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of block C_i , selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted. Related apparatus and methods are also provided.

WO 2004/086664 A3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IL04/00144

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 1/100, 9/100; G06F 11/30

US CL : 380/28,29,37,265; 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/28,29,37,265; 713/200

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,578,150 B2 (LUYSTER) 10 June 2003 (10.06.2003)	1-30
A	WO 99/66669 A2 (RIVEST et al.) 23 December 1999 (23.12.1999)	1-30
A	EP 0 996 250 A2 (PATEL et al) 26 April 2000 (26.04.2000)	1-30
A	US 6,249,582 B1 (GILLEY) 19 June 2001 (19.06.2001)	1-30
A	US 4,731,843 A (HOLMQUIST) 15 March 1988 (15.03.1988)	1-30
A	US 4,229,818 A (MATYAS et al) 21 October 1980 (21.10.1980)	1-30

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search

14 September 2004 (14.09.2004)

Date of mailing of the international search report

08 NOV 2004

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (703) 305-3230

Authorized officer

Ayaz Sheikh

Telephone No. 703-305-9648